

(2) The SP must provide the Government with sufficient information to enable the Government to determine whether the SP is eligible to receive such information, and possesses the capability to provide appropriate protections for the GFI;

(3) Upon approval by the Government, the SP must enter into a legally binding agreement with the DIB participant (and also an appropriate agreement with the Government in any case in which the SP will receive or share information directly with the Government on behalf of the DIB participant) under which the SP is subject to all applicable requirements of this part and of any supplemental terms and conditions in the DIB participant's FA with the Government, and which authorizes the SP to use the GFI only as authorized by the Government.

(k) The DIB participant may not sell, lease, license, or otherwise incorporate the GFI into its products or services, except that this does not prohibit a DIB participant from being appropriately designated an SP in accordance with paragraph (j) of this section.

#### **§ 236.5 Cyber security information sharing.**

(a) *GFI.* The Government shall share GFI with DIB participants or designated SPs in accordance with this part.

(b) *Initial incident reporting.* The DIB participant shall report to DC3/DCISE cyber incidents involving covered defense information on a covered DIB system. These initial reports will be provided within 72 hours of discovery. DIB participants also may report other cyber incidents to the Government if the DIB participant determines the incident may be relevant to information assurance for covered defense information or covered DIB systems or other information assurance activities of the Government.

(c) *Follow-up reporting.* After an initial incident report, the Government and the DIB participant may voluntarily share additional information that is determined to be relevant to a reported incident, including information regarding forensic analyses, mitigation and remediation, and cyber intrusion damage assessments.

(d) *Cyber intrusion damage assessment.* Following analysis of a cyber incident, DC3/DCISE may provide information relevant to the potential or known compromise of DoD acquisition program information to the Office of the Secretary of Defense's Damage Assessment Management Office (OSD DAMO) for a cyber intrusion damage assessment. The Government may provide DIB participants with information regarding the damage assessment.

(e) *DIB participant attribution information.* The Government acknowledges that information shared by the DIB participants under this program may include extremely sensitive proprietary, commercial, or operational information that is not customarily shared outside of the company, and that the unauthorized use or disclosure of such information could cause substantial competitive harm to the DIB participant that reported that information. The Government shall take reasonable steps to protect against the unauthorized use or release of such information (e.g., attribution information and other nonpublic information) received from a DIB participant or derived from such information provided by a DIB participant, including applicable procedures pursuant to paragraph (h) of this section. The Government will restrict its internal use and disclosure of attribution information to only Government personnel and Government support contractors that are bound by appropriate confidentiality obligations and restrictions relating to the handling of this sensitive information and are engaged in lawfully authorized activities.

(f) *Non-attribution information.* The Government may share non-attribution information that was provided by a DIB participant (or derived from information provided by a DIB participant) with other DIB participants in the DIB CS/IA program, and may share such information throughout the Government (including with Government support contractors that are bound by appropriate confidentiality obligations) for cyber security and information assurance purposes for the protection of Government information or information systems.

(g) *Electronic media.* Electronic media/files provided by DIB participants to DC3 under paragraphs (b), (c) and (d) of this section are maintained by the digital and multimedia forensics laboratory at DC3, which implements specialized handling procedures to maintain its accreditation as a digital and multimedia forensics laboratory. DC3 will maintain, control, and dispose of all electronic media/files provided by DIB participants to DC3 in accordance with established DoD policies and procedures.

(h) *Freedom of Information Act (FOIA).* Agency records, which may include qualifying information received from non-federal entities, are subject to request under the Freedom of Information Act (5 U.S.C. 552) (FOIA), which is implemented in the Department of Defense by DoD Directive 5400.07 and DoD Regulation 5400.7-R (see 32 CFR parts 285 and 286, respectively). Pursuant to established procedures and applicable regulations, the Government will protect sensitive nonpublic information under this Program against unauthorized public disclosure by asserting applicable FOIA exemptions, and will inform the non-Government source or submitter (e.g., DIB participants) of any such information that may be subject to release in response to a FOIA request, to permit the source or submitter to support the withholding of such information or pursue any other available legal remedies.

#### § 236.6 General provisions.

(a) Confidentiality of information that is exchanged under this program will be protected to the maximum extent authorized by law, regulation, and policy.

(b) The Government and DIB participants will conduct their respective activities under this program in accordance with applicable laws and regulations, including restrictions on the interception, monitoring, access, use, and disclosure of electronic communications or data. The Government and the DIB participant each bear responsibility for their own actions under this program.

(c) Prior to sharing any information with the Government under this program pursuant to the FA, the DIB par-

ticipant shall perform a legal review of its policies and practices that support its activities under this program, and shall make a determination that such policies, practices, and activities comply with applicable legal requirements. The Government may request from any DIB participant additional information or assurances regarding such DIB participant's policies or practices, or the determination by the DIB participant that such policies or practices comply with applicable legal requirements.

(d) This voluntary DIB CS/IA program is intended to safeguard covered defense information. None of the restrictions on the Government's use or sharing of information under the DIB CS/IA program shall limit the Government's ability to conduct law enforcement, counterintelligence activities, or other activities in the interest of national security; and participation does not supersede other regulatory or statutory requirements.

(e) Participation in the DIB CS/IA program is voluntary and does not obligate the DIB participant to utilize the GFI in, or otherwise to implement any changes to, its information systems. Any action taken by the DIB participant based on the GFI or other participation in this program is taken on the DIB participant's own volition and at its own risk and expense.

(f) A DIB participant's voluntary participation in this program is not intended to create any unfair competitive advantage or disadvantage in DoD source selections or competitions, or to provide any other form of unfair preferential treatment, and shall not in any way be represented or interpreted as a Government endorsement or approval of the DIB participant, its information systems, or its products or services.

(g) The DIB participant and the Government may each unilaterally limit or discontinue participation in this program at any time. Termination shall not relieve the DIB participant or the Government from obligations to continue to protect against the unauthorized use or disclosure of GFI, attribution information, contractor proprietary information, third-party proprietary information, or any other information exchanged under this program,